J Comput Virol Hack Tech (2016) 12:121–123
DOI 10.1007/s11416-016-0275-1

EDITORIAL

Knowledge-based System and Security

Yu-Keum Jeong[1] · **Roy C. Park**[2]

Published online: 11 May 2016

Welcome to this special issue of the Journal of Computer Virology and Hacking Techniques on Knowledge-based System and Security. The main goal for this special issue is to be a timely vehicle for publishing selected research papers from academia and practitioners in different industries on this emerging topic. Knowledge-based security systems are developed to ensure computer virology-making by effectively using timely and appropriate knowledge base, security management, hacking techniques for convergence [11–14]. This special issue covers some of the hottest topics in knowledge-based system and security, including: Privacy and authentication for wireless network; Convergence security in ubiquitous computing; Algorithmic and computer virology; Innovative applications of ubiquitous computing; Intelligent applications for security processing; Hacking, Knowledge processing algorithms; User experience in knowledge security systems, embedded systems security; Personalization, privacy, computer virology, Information indexing; computer virology; Cryptology and embedded systems; Security applications in computer virology.

The paper by Lee [1] presents a secure game development method for the Internet of Things (IoT). The proposed method for developing a game in the IoT service environment looks at the length-related password vulnerability and introduces a method with which a hacker lures Internet users and seizes the users' IDs and passwords, as well as their password generation patterns. An additional improved process is necessary to prevent various attacks, like seizing the account. The proposed method shows that finding a pattern with collected passwords and speculating about the user's password is possible. Seizing the user's PIN for authentication certificates and for financial information on other sites is possible. The paper by Ferrand et al. [2] presents combinatorial detection of malware by import address table (IAT) discrimination. This study presents a new technique that helps proactively detect malware without any prior update of either the engine or the relevant databases. The main focus is the ability to concentrate the information inside combinatorial design blocks, and hence, exhibit correlations between IAT functions at a far higher order. The proposed technique was implemented in the French antivirus software initiative, Démonstrateurs d'Antivirus Français et Internationaux (DAVFI), and was intensively tested on real cases, confirming the detection performance.

The paper by Hong [3] presents two-channel user authentication by using a universal serial bus (USB) for the cloud. He developed USB authentication for vulnerable communications environments. The proposed solution is a new generic multi-factor authentication protocol that authenticates users by password with a USB. This method has significant advantages in terms of computation and communications over another generic design. Hong expects the new protocol to become a promising authentication solution for unsecured connections. The contribution is stand-alone authentication, with which users can be authenticated correctly even if the connection to the remote authentication server is down. He provides an efficient and controllable design for stand-alone authentication for any multi-actor authentication protocol. The paper by Kim et al. [4] presents a secure analysis of a vehicular authentication security scheme (VASS) for RSUs in a vehicular ad hoc network (VANET). They present a vehicular authentication security scheme for highways using

✉ Roy C. Park
parkc.roy@gmail.com

[1] Strategy Department, Society of Digital Policy & Management, Daewoo Plaza 301, Dujeong-ro 240, Cheonan-si, Chungcheongnam-do, Republic of Korea

[2] Division of Computer Engineering, Dongseo University, 47, Jurye-ro, Sasang-gu, Busan 617-716, Republic of Korea

an encoded algorithm and time random numbers for mutual authentication using a Petri Net. As such, Petri Net modeling helps to smoothly cope with defining and implementing security requests in a VANET complicated by many changes in vehicles. Performance results show that the computation effort is much lower than other methods in the hash functions, and the VASS has security properties such as privacy, authentication, and prevention of Sybil attacks. They will extend the scheme to vehicle-to-infrastructure communications based on reduced costs and communications message volume.

The paper by Kim et al. [5] presents a study of the effects of security risks on acceptance of enterprise cloud services, moderating employment and non-employment using partial least squares (PLS) multiple group analysis. This paper analyzes the effects of security risk factors fit for the cloud computing paradigm on the acceptance of enterprise cloud services with the intent to illuminate factors for vitalizing the adoption of corporate cloud services in the future. Acceptance intention was set as a dependent variable. Independent variables were set in reference to the technology acceptance theory. Security risks were categorized into compliance risk, information leakage risk, troubleshooting risk, and service discontinuation risk in order to design a model for analysis. The paper by Kang et al. [6] proposes a two-channel authentication technique using cardiac impulse-based one-time pads. This study examined an authentication technique that combines real-time time information and cardiac impulses. This is an authentication technique that is safe against third-party attacks and is convenient, enabling immediate payment as soon as the user inputs the password. Authentication techniques with two characteristics of security and convenience should be more available. An authentication technique will be developed that applies various biometrics to FinTech Security–like facial recognition.

The paper by Kim et al. [7] proposes an over-the-top (OTT) user authentication system by age classification. The proposed method develops a system to restrict viewing by adolescents of inappropriate broadcasts, linking them with a content database system inside an OTT device. This study looks at an age-recognition method based on the characteristics of wrinkles or of skin information on the face. The size and depth of wrinkles and skin and their orientation are efficiently reflected by employing Gabor filters. It is necessary to detect robust features of such characteristics from a variable image influenced by the quality of the image, the expression, lighting, and pose. Additional studies to control the OTT with voice and motion are also demanded. The paper by Kim et al. [8] introduces an analysis of secure coding using a symbolic execution engine. They present security vulnerabilities through white-box/black-box analyses and enhanced security vulnerability inspection. A static analysis methodology that can inspect all sources is the recommended methodology. If it can dramatically reduce false positives and false negatives, it will be far better, and can eliminate most vulnerabilities. In the use of data from a symbolic execution engine, when the software is terminated abnormally or exposed to risk, they can create an autorun script and use it to prove security vulnerabilities.

The paper by Dechaux et al. [9] proposes a proactive defense against malicious documents: formalization, implementation and case studies. The purpose is to show that is it possible to proactively manage known and unknown threats. The aim is to provide finer analysis to categorize the level of maliciousness, thus enhancing prevention by selectively removing the truly malicious parts in a document. This study presents a new prevention model and new techniques to proactively process potentially malicious office documents. This approach no longer needs prior knowledge of malicious inside features (known or unknown), and keeps the user from accessing the document's content. The paper by Mun et al. [10] suggests a blackhole attack: a user-identity and password-seizure attack using a honeypot. A scenario created by an advanced method of the blackhole attack is introduced. The method shows that finding a pattern in collected passwords and speculating about the user's password is possible. Seizing the user's PIN for an authentication certificate and financial information from other sites is possible. Users would not even notice if an attack had happened if they are redirected from the modified site to the real site after exceeding the maximum number of login attempts, which is usually only two or three times. Thus, various and evolved attacks are possible.

This fine collection of papers was achieved by fruitful collaborations. We wish to thank all the authors for their contributions and the reviewers for assisting our editorial work. We do hope that the papers included in this issue will satisfy the audience of the Journal of Computer Virology and Hacking Techniques and readers will find them interesting. Furthermore, we would like to thank Professor Eric Filiol, editor-in-chief of the Journal of Computer Virology and Hacking Techniques, for his valuable remarks and his undeterred help throughout the publication process.

References

1. Lee, M.J.: Secure game development for IoT environment. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-015-0255-x
2. Ferrand, O., Filiol, E.: Combinatorial detection of malware by IAT discrimination. J. Comput. Virol. Hacking. Tech. (2016). doi:10.1007/s11416-015-0257-8
3. Hong, S.H.: Two-channel user authentication by using USB on Cloud. J. Comput. Virol. Hacking. Tech. (2016). doi:10.1007/s11416-015-0254-y
4. Kim, Y.C., Lee, J.K.: A secure analysis of vehicular authentication security scheme of RSUs in VANET. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-016-0269-z

5. Kim, D.Y., Li, G., Park, S.T., Ko, M.H.: A study on effects of security risks on acceptance of enterprise cloud service: moderating of employment and non-employment using PLS multiple group analysis. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-015-0262-y
6. Kang, B.S., Lee, K.H.: 2-Channel authentication technique using cardiac impulse based OTP. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-016-0271-5
7. Kim, K.Y., Park, B.J., Suh, Y., Park, J.: OTT user authentication system by age classification. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-016-0268-0
8. Kim, J.H., Ma, M.C., Park, J.P.: An analysis on secure coding using symbolic execution engine. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-016-0263-5
9. Dechaux, J., Filiol, E.: Proactive defense against malicious documents: formalization, implementation and case studies. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-015-0259-6
10. Mun, H.J., Han, K.H.: Blackhole attack: user identity and password seize attack using honeypot. J. Comput. Virol. Hacking Tech. (2016). doi:10.1007/s11416-016-0270-6
11. Chung, K., Boutaba, R., Hariri, S.: Knowledge based decision support system. Inform. Technol. Manag. **17**(1), 1–3 (2016)
12. Jo, S.M., Chung, K.: Design of access control system for telemedicine secure XML documents. Multimed. Tools Appl. **74**(7), 2257–2271 (2015)
13. Kim, S.H., Chung, K.: Emergency situation monitoring service using context motion tracking of chronic disease patients. Clust. Comput. **18**(2), 747–759 (2015)
14. Chung, K.: Recent trends on convergence and ubiquitous computing. Pers. Ubiquitous Comput. **18**(6), 1291–1293 (2014)